REMARKS

Applicant has carefully reviewed and considered the Office Action mailed on April 16, 2007, and the references cited therewith.

Claims 1,2, 4-5, 9-10, 13, 15-16, and 18-19 are amended, claims 2-33, 10-12, 14 -17 are canceled, and claims 21-22 are added; as a result, claims 1,4-9,13,15, and 18-22 are now pending in this application. The amendments to the claims are supported by the description, claims, and drawings of the subject application as originally filed. Thus, no new matter is added by the amendments.

§102 Rejection of the Claims

Claims 1-6 and 7-19 were rejected under 35 USC §102(e) as being anticipated by as being anticipated by Gilchrist U.S. Pat. No. 6950949 (hereinafter "Gilchrist").

Amended claim 1 includes the following limitations:

> A method performed by a client comprising:
> storing a secret in a secure storage;
> receiving a password challenge from a server; and
> responsive to the password challenge calling a secure password prompt routine which accesses the secret in the secure storage, generates an authentication graphic based on the secret, and displaying a prompt asking a user for a password, the prompt including an the authentication graphic which is visible to the user; wherein the secure password prompt routine displays the authentication graphic for all password challenges, there being no requirement of an association between the server and the authentication graphic.

(Claim1, emphasis added)

In the system of Gilchrist, dynamic password legitimacy information 112 is stored in a memory 108. The memory 108 is not disclosed as being a secure storage. In use, when a password prompt command is detected, the system retrieves the associated dynamic password entry interface legitimacy information from the memory 108 (emphasis added). The dynamic password entry interface legitimacy information is displayed together with a password entry interface 116. After a user enters a password, the password is verified and the user is granted access to a protected process, device, or information on the system (See Figures of 3 and 4, and associated description). The system of Gilchrist requires an association to be created between the dynamic password entry interface legitimacy information and an application that requires entry any of a password to gain access to protected information. This is described in Gilchrist Column 7 lines 19-25 where during initialization the user selects an image which is stored in the memory 108 for that user and for a particular application.

It follows therefore, that an application for which an association has not been created will display a password prompt without the dynamic password entry interface legitimacy information. In such a case, the user would not enter password information as the absence of the dynamic password entry interface legitimacy information would be a clue to the user not to trust the application. In contrast to the system of Gilchrist, claim 1 recites that there is no requirement between the server making the password challenge and the authentication graphic. This greatly enhances the utility of the present invention, as the user does not have to make an association between each application requesting password information and the authentication graphic. For example, take the case of a user who visits an arbitrary website requiring password information for secure access. In the case of the inventive system of the present application, without any prior association between the website and the authentication graphic, the secure password prompt routine would access the secure storage and generate an authentication graphic which would be displayed together with a password prompt. The visibility of the authentication graphic together with the password prompt would signify to the user that the secure password prompt routine is operational. The user can then input password information without fear of misuse thereof because the user knows that the secure password prompt routine would encrypt the password information prior to transmission thereof to the arbitrary website. If the system of

Gilchrist were used to visit an arbitrary website, since the website would have no association with dynamic password entry interface legitimacy information, such information would not be shown with a password prompt from the arbitrary website. In such a case, a user of the system would not enter password information as the password prompt cannot be trusted. The user would thus first have to create an association between the website and dynamic password entry interface legitimacy information.

Moreover, in the system of Gilchrist, the dynamic password entry interface legitimacy information is not stored in a secure storage. Thus, a malicious program can gain access to the dynamic password entry interface legitimacy information and display it to the user in order in induce the user to input password information.

Based on the foregoing, it is respectfully submitted that Gilchrist does not teach or suggest all limitations of claim 1 and thus cannot anticipate claim 1.

Independent claims 9 and 15 include limitations similar in scope to the above-described limitations of claim 1. Thus, it is respectfully submitted that these claims are also not anticipated by Gilchrist.

Given that claims 4-8, 21-22, 13, and 18-20 depend on one of claims 1, 9, and 15 respectively, it is respectfully submitted that these claims are also not anticipated by Gilchrist.

§103 Rejection of the Claims

Claims 6 and will 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilchrist in view of Kobata et al. U.S. Pub. No. 20060005237 (hereinafter "Kobata"). Applicant traverses.

In the system of Gilchrist, a password entry method is described whereby entry is gained to a protected process, device, or information. A password in input to the system after the system displays a password prompt with dynamic password entry interface legitimacy information. The password is verified by the system before granting access to the protected process, device, or information. The system does not transmit or send the password to any other entity. That being the case the Examiner would agree that there is no need in the system of Gilchrist to encrypt the password. Thus, of ordinary skill in the art would not be motivated to combine Kobata and Gilchrist as suggested by the Examiner as there would be no advantage or benefit to doing so. In this regard, Applicant respectfully submits that the Examiner has failed to make a *prima facie* case of obviousness as he is required to do.

Accordingly, it is respectfully submitted that claims 6, and 20 are not obvious in view of Gilchrist and Kobata.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (650-903-2257) to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 503437

Respectfully submitted,

MICHAEL J TOUTONGHI

By his Representatives,

Hahn and Moodley LLP
P.O. Box 52050

650-903-2257

Date 9/17/2007

By /Vani Moodley/

Vani Moodley
Reg. No. 56631